BRADLEY/GROMBACHER, LLP
Marcus J. Bradley, Esq. (SBN 174156)
Kiley L. Grombacher, Esq. (SBN 245960)
Lirit A. King, Esq. (SBN 252521)
31365 Oak Crest Drive, Suite 240
Westlake Village, California 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
E-Mail: mbradley@bradleygrombacher.com
kgrombacher@bradleygrombacher.com
lking@bradleygrombacher.com

Attorneys for Plaintiffs
(Additional counsel on next page)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JUAN FLORES-MENDEZ, an individual and TRACY GREENAMYER, an individual, on behalf of classes of similarly situated individuals,

Plaintiffs,

v.

ZOOSK, INC., a Delaware corporation,

Defendant.

Case No: 3:20-cv-04929-WHA

PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFF'S MOTION FOR CLASS CERTIFICATION

Hon. William Alsup
Date: July 7, 2022
Time: 8:00 a.m.
Courtroom 12, 19th Floor

Additional Counsel for Plaintiffs and the Putative Class:

CROSNER LEGAL P.C.
Zachary M. Crosner (SBN 272295)
Michael R. Crosner (SBN 41299)
433 N. Camden Dr., Suite 400
Beverly Hills, CA 90210
Telephone: (310) 496-4818
Facsimile: (310) 510-6429
Email: zach@crosnerlegal.com
mike@crosnerlegal.com

MORGAN & MORGAN COMPLEX LITIGATION GROUP (*Admitted Pro hac Vice*)
John A. Yanchunis (FL Bar No. 234681)
Ryan McGee (FL Bar No. 64957)
201 N Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Email: jyanchunis@forthepeople.com
rmcgee@forthepeople.com

TABLE OF CONTENTS

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 2

A. Zoosk's Background and Acquisition by Spark 3

B. Zoosk [redacted]" and "Noticed" the Breach 4

C. The Breach Investigation and Response was Bungled 5

D. Zoosk's Remediation and Ongoing Processes are Inadequate and Incomplete 8

E. Zoosk's Various Other Security Failings 8

III. LEGAL STANDARD 10

IV. ARGUMENT 11

A. THE PROPOSED CLASSES MEET RULE 23(a) REQUIREMENTS 11

1. With [redacted] Users Breached, Numerosity is Met 11

2. Zoosk's Conduct Related to The Breach Raises Common Legal and Factual Questions 12

3. Plaintiff's Claims are Typical of the Class 13

4. Plaintiff and Proposed Class Counsel are Adequate 13

B. THE COURT SHOULD CERTIFY A 23(b)(2) CLASS 14

C. RULE 23(b)(3) CERTIFICATION OF THE SUBSCRIPTION SUBCLASS IS PROPER 16

1. Common Questions of Law and Fact Predominate 17

2. A Class Action is Superior to Millions of Expensive Trials 22

D. THE COURT SHOULD ALSO CERTIFY COMMON ISSUES UNDER RULE 23(C)(4) 23

V. CONCLUSION 25

TABLE OF AUTHORITIES

Cases

Amgen Inc. v. Conn. Ret. Plans & Tr. Funds,
133 S. Ct. 1184 (2013) 10, 18

Brazil v. Dole Packaged Foods, LLC,
2014 WL 2466559, (N.D. Cal. May 30, 2014) 14

Briseno v. Con Agra Foods, Inc.,
844 F. 3d 1121 (9th Cir. 2017). 11, 23

Davis v. HSBC Bank Nevada, N.A.,
691 F.3d 1152 (9th Cir. 2012). 17

Deane v. Fastenal Co.,
2012 WL 12552238 (N.D. Cal. Sept. 26, 2012 24

Ellsworth v. U.S. Bank, N.A.,
2014 WL 2734953 (N.D. Cal. June 13, 2014). 17

Giroux v. Essex Prop. Tr., Inc.,
2018 WL 2463107 (N.D. Cal. June 1, 2018); 17

Hanlon v. Chrysler Corp.,
150 F.3d 1101 (9th Cir. 1998). 13

In re Adobe Sys., Inc. Privacy Litig.,
66 F. Supp. 3d 1197 (N.D. Cal. 2014); 19

In re Brinker Data Incident Litig.,
3:18-CV-686-TJC-MCR, 2021 WL 1405508 (M.D. Fla. Apr. 14, 2021) 12, 22

In re Deepwater Horizon,
739 F.3d 790 (5th Cir. 2014); 23

In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,
19-MD-2879, 2022 WL 1396522 ..... 12, 22, 24

In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig.,
722 F.3d 838 6th Cir. 2013) 23

In re Yahoo! Inc. Customer Data Sec. Breach Litig.,
No. 16-md-02752-LHK, 2017 WL 3727318, (N.D. Cal. Aug. 30, 2017 ..... 10, 14, 19

Jimenez v. Allstate Ins. Co.,
765 F.3d 1161 (9th Cir. 2014) 23, 24

Just Film v. Buono,
847 F.3d 1108 (9th Cir. 2017). 17

Kamakahi v. Am. Soc'y for Reprod. Med.,
305 F.R.D. 164, 193 (N.D. Cal. 2015) 24

Kumar v. Salov N. Am. Corp.,
2016 WL 3844334 18

Lanovaz v. Twinings N. Am., Inc.,
2014 WL 1652338 (N.D. Cal. Apr. 24, 2014). 18

Lilly v. Jamba Juice Co.,
308 F.R.D. 231 (N.D. Cal. 2014) 18

Loritz v. Exide Techs., Inc.,
2015 WL 6790247 (N.D. Cal. July 21, 2015) 24

Parsons v. Ryan, 7
54 F.3d 657 (9th Cir. 2014) 15

Rannis v. Recchia,
380 F. App'x 646 (9th Cir. 2010) 11

In re Lenovo Adware Litig.,
2016 WL 6277245 (N.D. Cal. Oct. 27, 2016) 16

Smith v. Triad of Alabama, LLC,
2017 WL 1044692 (M.D. Ala. Mar. 17, 2017) 17

Soares v. Flowers Foods, Inc.,
320 F.R.D. 464 (N.D. Cal. 2017) 22

Staton v. Boeing Co.,
327 F.3d 938 (2003) 13

Tasion Commc'ns, Inc. v. Ubiquiti Networks, Inc.,
308 F.R.D. 630 (N.D. Cal. 2015). 23

Torres v. Mercer Canyons Inc.,
835 F. 3d 1125 (9th Cir. 2016). 12

Wal-Mart Stores, Inc. v. Duke
564 U.S. 338 (2011) 14

Williams v. Gerber Prods. Co.,
552 F.3d 934 (9th Cir. 2008) 17

Rules

Federal Rule of Civil Procedure Rule 23(b)(2). 1, 10, 11, 14, 15

Federal Rule of Civil Procedure Rule 23(a)(4) 13

Federal Rule of Civil Procedure Rule 23(b)(3)(A) 22

I. INTRODUCTION

Defendant, Zoosk, Inc. ("Zoosk")—an online dating service—lost millions of consumers' personally identifiable information ("PII") in a data breach that the hackers openly bragged was "not too hard" to execute. (ECF No. 191, Fourth Amended Complaint ("FAC"), ¶ 5). Among the PII looted were class members' names, email addresses, dates of birth, demographical information, gender, and gender search preferences. FAC, ¶ 8. Notably, Zoosk did not detect the breach or exfiltration, rather; it was brought to Zoosk's attention by third parties. FAC, ¶¶ 4–6, 14.

Zoosk's negligence caused this harm. Zoosk failed to implement reasonable and appropriate security measures that could have prevented the breach—namely, the timely and periodic rotation of access key credentials, the use of available intrusion detection services, and the lack of appropriate priority being given to information security generally and the intrusion at issue here specifically at the time it occurred.

Plaintiff Tracy Greenamyer[1] seeks class certification of her claims for negligence and violation of California's Unfair Competition Law (UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*., which are naturally suited for resolution on a classwide basis. Discovery here shows how the Breach uniformly affected consumers, the groups of consumers involved, and the types of PII released. Plaintiff and class members were injured by the same Breach. Because Zoosk's data security practices uniformly apply to all class members, certification under Rule 23(b)(2) is unquestionable proper, and, for the same reason, common issues will predominate in the trial of all claims arising from the Breach. Class treatment is superior as individual consumers cannot be expected to present the technical documents and expert testimony needed to prove that Zoosk failed to provide reasonable and adequate data security, resulting in the Breach. Zoosk has both the means and responsibility to protect its users' PII. Finally, the remedies available to class members will also be common. The Court should certify Plaintiff's claims pursuant to Rule 23(b)(2) (as to

[1] As noted further below, this motion is brought on behalf of, and seeks appointment as class representative of, solely Plaintiff Greenamyer.

injunctive relief), 23(b)(3) (as to the Subscription Subclass), and/or 23(c)(4) for those who wish to prove out-of-pocket damages.[2]

II. FACTUAL BACKGROUND

As alleged in Plaintiff's complaint, users of Zoosk's services are required to provide Zoosk with their personally identifiable information, including names, email addresses, dates of birth, demographical information, gender, gender search preferences, and other sensitive and confidential information ("PII"). Since at least October 7, 2013, Zoosk has maintained a Privacy Policy that binds its users to certain obligations in exchange for Zoosk's promises that it will protect that PII and proactively prevent criminal and other unlawful activity. FAC, ¶¶ 34–48. On May 11, 2020, Zoosk "learned that an unknown third party claimed to have accessed certain Zoosk member information." FAC, ¶ 6. This discovery was not through the due diligence of Zoosk's information technology or security teams, but rather from an internet announcement from the hacking group ShinyHunters, which claimed that it was "not too hard" to access Zoosk's systems and exfiltrate millions of users' PII. FAC, ¶¶ 4–5. Put differently, Zoosk failed on its promises to securely maintain millions of users' PII, failed to detect, address, and remediate any malicious activity, and allowed unauthorized third parties to exfiltrate millions of users' PII.

Discovery in this case has only confirmed and buttressed those allegations. First, the fact of and scope of the Breach is not in dispute [redacted]. Zoosk's Amended Resp. to Plfs' 1st Interrog., Resp. No. 8, p. 15, attached as **Exhibit A**. [redacted], Conor Callahan, Zoosk's former Technical Lead–Platform & Infrastructure, [redacted]. *Id.* [redacted]. *Id.*

[2] Plaintiff acknowledges the Court's prior rulings on dark web value, pricing, and other monetary damages. (ECF No. 61). Due to the Court's prior rulings, Plaintiff's requested relief under Rule 23(b)(3) is limited to the scope of those rulings.

[3] EC2 refers to AWS's Elastic Compute Cloud, which are virtual computing environments. *See, e.g.*, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

at 16.

Zoosk's corporate representative confirmed that information corresponding to [redacted] Zoosk users was taken in the Breach, including [redacted]." Munoz Dep. Tr. 32:1–18, 91:8–24, attached as **Exhibit B**. Notably, [redacted]. Munoz Dep. Tr. 69:20–23. The corporate representative also confirmed that Zoosk "[redacted]." Munoz Dep. Tr. 104:19–23.[4] A more detailed factual narrative of Zoosk's discovery and response to the Breach, as well as its cybersecurity footing follows.

A. Zoosk's Background and Acquisition by Spark

The corporate context in which the Breach occurred is key in understanding the chaotic state of affairs at Zoosk at the time on the Breach in January 2020. Zoosk is a dating website/application, which began as an [redacted] Tuttle Depo. Tr. 18:7–19:24, attached as **Exhibit C**. In approximately [redacted], Zoosk [redacted] Tuttle Depo. Tr. 31:3–32:3.

In or about July of 2019, Zoosk was [redacted] Munoz Depo. Tr. 76:17–19; 100:25–102:20. [redacted] Munoz Depo. 101:5–14.

While even prior to the acquisition information security at Zoosk was suspect at best, in the wake of the purchase, it was abysmal. At the time of the Breach, Zoosk [redacted]. Tuttle Depo. Tr. 44:6–47:11; *see also* Callahan Depo. Tr. 91:10–20, attached as **Exhibit D**. The company did not have [redacted]

[4] *See also* Munoz Dep. Tr. 104:24–105:7 ("[redacted]

[redacted] Munoz Depo. Tr. 35:21–36:3; Tuttle 116:2–4 And the only pertinent [redacted]" Hoskins Depo Tr. 20:2–23, attached as **Exhibit E**.[5]

This left security responsibility in the hands of a skeleton crew of overwhelmed and undermotivated staff—primarily Messrs. Ethan Tuttle and Conor Callahan—both of whom, by the time of the Breach [redacted] Callahan Depo. Tr. 91:10–20; Tuttle Depo. Tr. 142:10–13. As Mr. Tuttle testified, after the acquisition, Zoosk was "[redacted]." Tuttle Depo. Tr. 130:22–24. Indeed, by the time of the Breach in January 2020, Mr. Tuttle, Zoosk's then Director/VP of Platform Security and Infrastructure,[6] viewed his job responsibilities as little more than "[redacted]." Tuttle Depo. Tr. 38:10–25.

B. Zoosk "[redacted]" and "Noticed" the Breach

Notably, not only was discovery of the exfiltration a happy accident, so was discovery of the Breach itself. Specifically, Mr. Tuttle testified that discovery of the Breach in the first instance was "[redacted]." Tuttle Depo. Tr. 74:5. Contemporaneous documents relay the same sentiment: "[redacted][.]" Tuttle Depo. Exh. 6, ZOOSK00001084 at 1085 (emphasis in original).[7] Indeed, the Breach was only discovered initially because Mr. Callahan, Zoosk's Technical Lead of Platform and Infrastructure[8] happened to "[redacted]." Callahan Depo. Tr. 30:23–25;[9] *see also* Kessler Depo. Tr. 17:10–14, attached as **Exhibit F,** ("[redacted]

[5] Mr. Hoskins candidly admitted that despite (a) not being employed by Zoosk directly, and (b) the complex web of entities at issue in this case, [redacted]. Hoskins Depo. Tr. 135:24–136:5.
[6] Munoz Depo. Tr. 37:19–25.
[7] All deposition exhibits cited to herein can be found following the end of the transcript—i.e. after the index—of the referenced deposition transcript.
[8] Munoz Depo. Tr. 23:2–3.
[9] "An Ec2 instance is a virtual server provided by Amazon or AWS." Callahan Depo. Tr. 31:3–4.

[redacted]

This indicated that the servers [redacted] Callahan Depo. Tr. 32:2–6. Notably, no alerts were triggered and/or observed, no intrusion detection system(s) alarmed, no monitoring was heeded, rather, a Zoosk employee simply "[redacted] and happened to [redacted]. *See* Decl. of Matthew Strebe, ¶¶ 96–101, 104, attached as **Exhibit G**.

C. The Breach Investigation and Response was Bungled

Given this milieu it is little surprise that the investigation into the incident was equally beguiled. To this day, Zoosk purports to "[redacted]." Zoosk's Amended Resp. to Plfs' 1st Interrog., Resp. No. 8, p. 14.

Nonetheless, it is undisputed that the Breach occurred because an [redacted]. *Id*. at p. 15. Zoosk claims that it [redacted]," but also admits that it "[redacted] . . . ." *Id*.

Even so, Grant Kessler—the Team Lead, Platform Security and Head of Security at Spark—testified that the access key used in the Breach was taken from either (1) the [redacted], or (2) certain [redacted]).[10] Notbaly, Mr. Kessler wrote, candidly, in the immediate wake of the Breach that "[redacted]" Kessler Depo. Exh. 63, ZOOSK00000183 at 184; Kessler Depo. Tr. 54:21– 64:21.

Regardless of how the access key was in fact obtained, Zoosk had failed to rotate the access

[10] Kessler Depo. Tr. 66:22–73:10 ("[redacted]).

key used in the attack [redacted], despite an internal policy requiring [redacted]. Kessler Depo. Tr. 122:19–25, Tuttle Depo. Tr. 84:4–18. This failure was on account of self-described [redacted].” Hoskins Depo. Exh. 33, ZOOSK00000102; Kessler Depo. Tr. 123:9–124:24.[11]

Zoosk concedes that, “[redacted]”:

[redacted].”

Zoosk’s Amended Resp. to Plfs’ 1st Interrog., Resp. No. 8, p. 15. It was this [redacted]. *Id.*

Yet, resort to solely AWS CloudTrail data underscores Zoosk’s data security inadequacies and is the ***first*** example of Zoosk’s bungled investigation. [redacted] had not been enabled[12] (as also shown by the fact that enabling them was one of Zoosk’s main remediation steps).[13] This near exclusive reliance on CloudTrial was woefully misplaced, however, because it fails to account for the situation in which the exfiltrated data is simply moved to another AWS account owned by the attacker. In that scenario, Zoosk’s CloudTrial logs would not reflect the transfer, rather only the receiving account’s CloudTrial logs would. *See* Strebe Decl. ¶¶ 37, 48–49,

---

[11] *See also* Kessler Depo. Exh. 76, ZOOSK00000175 (“[redacted]”) (emphasis added).

[12] Depo. Kessler Exh. 67, ZOOSK00001555 (“[redacted].”); Kessler Depo. Tr. 102:15–103:3; Depo. Exh. 58, ZOOSK00001563 (“[redacted]”); Kessler Depo. Exh. 68, ZOOSK00000263 (“[redacted] Kessler Depo. Tr. 52:19–54:15, 102:15–104:, 110:3–113:11.

[13] Hoskins Depo. Ex. 47, ZOOSK00000384 (“[redacted].]”); Kessler Depo. Tr. 22:24–24:17.

113–117, 121. Two of the individuals most directly responsible for investigation of the Breach—Messrs. Kessler and Callahan—were both unaware of this elementary scenario. Kessler Depo. Tr. 76:24–78:4; Callahan Depo Tr. 133:3–15. Indeed, Mr. Kessler testified that he "[redacted] and that the [redacted] Kessler Depo. Tr. 76:7, 81:2 This easily explains why Zoosk was unaware its customers data had been exfiltrated at the time of the Breach in January 2020: it did not know where or how to look.

While AWS's GuardDuty service likely would have logged both the creation and the use of access keys to grant public permission (or specific permission for any 3rd party AWS account to access Zoosk's account), (Strebe Decl. ¶¶ 99–100), Zoosk had [redacted].[14] [redacted], once again it was too little, too late.

Second, Zoosk did not utilize a professional incident response team or engage AWS's Professional Services beyond what its AWS account manager was willing to provide without additional cost. Rather Zoosk relied exclusively on internal employees without [redacted]. Callahan Depo. Exh. 28; Strebe Decl. ¶¶ 108–112; Callahan Depo. Tr. 11:8–17 ("Q. [redacted]. "); Tuttle Depo. Tr. 11:2–12:14.

Third, Zoosk's information security team [redacted],[15] [redacted]. Strebe Decl. ¶¶ 51, 59. Consequently, as noted above, even today, Zoosk [redacted], thus, leaving any

[14] Kessler Depo. Exh. 58, ZOOSK00001563 ("[redacted].]"); Callahan Depo. Tr. 34:16–35:1 ([redacted] Munoz Depo. Tr. 50:6–9 ("[redacted].").

[15] Zoosk's Amended Resp. to Plfs' 1st Interrog., Resp. No. 8, p. 16; Kessler Depo. Tr. 28:2–30:8.

attempted remediation uncertain, at best.

D. Zoosk's Remediation and Ongoing Processes are Inadequate and Incomplete

Zoosk's remediation efforts consisted of a [redacted] ." Munoz Depo Tr. 70:7–72:23; *see also id.* 93:17–94:13 (stating [redacted]).

However, Zoosk's [redacted] was, at most, incomplete and delayed as its third-party, [redacted] .[16] [redacted] was likewise incomplete and delayed. While Zoosk has asserted this was done essentially contemporaneously with discovery of the Breach,[17] other evidence shows [redacted] . Strebe Decl. ¶ 50; Hoskins Depo. Exh. 48 at ZOOOSK00000414; Kessler Depo Tr. 116:18–117:9.

Moreover, despite this history of abject failures, Zoosk has not engaged in any routine [redacted] . Strebe Decl. ¶ 137; Munoz Depo. Tr. 56:23–57:10, 83:1–15

E. Zoosk's Various Other Security Failings

In addition to the many security failings directly contributing to, or following the Breach, Zoosk failed to implement or follow many other industry standard practices. Strebe Decl. ¶¶ 3, 84–94. For example, Zoosk failed to implement standard [redacted]

[16] *See* Strieb Decl. ¶¶ 70, 134; Callahan Depo. Exh. 23 at ZOOOSK00001119 ("[redacted] "); Callahan Depo Tr. 146:2–15.

[17] Munoz Depo. Tr. 22:21–23:7; Zoosk's Amended Resp. to Plfs' 1st Interrog., Resp. No. 8, p. 15 [redacted] .").

[redacted], *e.g.*, Callahan Depo. Tr. 30:1-9, and that were so [redacted]. Kessler Depo. Exh. 74, ZOOSK00001176; Kessler Depo. Exh. 58, ZOOSK00001563 at 1564; Kessler Depo. Tr. 71:4–73:5, 141:5–143:15.[18]

Zoosk maintained [redacted] than it needed to or should have. Rather, Zoosk maintained user's PII [redacted]. *See* Hoskins Depo. Exh. 32, ZOOSK0000111–113; *see also* Hoskins Depo. Tr. 42:17–49:15. Zoosk apparently had no policy or practice of reviewing data [redacted]. This greatly increased the number of individuals affected by the Breach and for no defensible business purpose. Strebe Decl. ¶ 87.

Zoosk maintained multiple inadequate and outdated [redacted]. Kessler Depo. Exh. 70, ZOOSK00000203–04, Kessler Depo. Exh. 71, ZOOSK00000398–99, Kessler Depo. Exh. 73, ZOOSK00000477; Kessler Depo. Tr. 128:14–133:19, 136:11–138:3. Those responsible were aware that [redacted]. Tuttle Depo. Tr. 53:13–24; Hoskins 52:18–24.

Zoosk did not [redacted]. Munoz Depo. Tr. 69:20–23. If it had, significant harms could have been prevented even in the event that the database was stolen, as it was here. Strebe Decl. ¶ 94.

Zoosk lacked useful [redacted], which led directly to the Breach. Hoskins Depo. Exh. 33; Kessler Depo. Tr. 124:5–11; Strebe Decl. ¶ 90.

Zoosk failed to use [redacted]

[18] Given this issue impacted the [redacted] was also located, this issue may have directly caused the Beach, as noted above.

[redacted]

Strebe Decl. ¶ 73.

And, prior to the Breach, [redacted]. Kessler Depo. Exh. 75, ZOOSK00001288–93; Tuttle Depo. Tr. 143:2–144:13.

III. LEGAL STANDARD

To certify a class under Federal Rule of Civil Procedure 23, a plaintiff must demonstrate numerosity, commonality, typicality, and adequacy, and satisfaction of the requirements for one of the class types defined in Rule 23(b). *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 979–80 (9th Cir. 2011). To certify a Rule 23(b)(2) class, the plaintiff must show that "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). Certification under Rule 23(b)(3) requires that "'questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.'" *Sali v. Corona Reg'l Med. Ctr.*, 889 F.3d 623, 629 (9th Cir. 2018). Rule 23(c)(4) provides the court with discretion to certify a class to resolve particular issues, such that "[e]ven if the common questions do not predominate over the individual questions," a court may "isolate the common issues . . . and proceed with class treatment of these particular issues." *Valentino v. Carter-Wallace, Inc.*, 97 F.3d 1227, 1234 (9th Cir. 1996).

A "'rigorous analysis'" is required, *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 586 (N.D. Cal. 2015), but this does not require or warrant "a mini-trial." *Sali*, 889 F.3d at 631. Nor is the district court "limited to considering only admissible evidence in evaluating whether Rule 23's requirements are met." *Id.* at 632. Where the merits are probed, they may be so only to the extent "that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Amgen Inc. v. Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455, 466 (2013). Plaintiff meets her burden under Rule 23, such that certification of the proposed Classes is warranted.

IV. ARGUMENT

Plaintiff seeks certification of the following classes:

- **Nationwide Class**: All individuals in the United States whose PII was compromised in the Data Breach announced by Zoosk on June 3, 2020; (as to injunctive relief under Rule 23(b)(2) and issue certification under Rule 23(c)(4));
- **Subscription Subclass**: All individuals in the United States whose PII was compromised in the Data Breach announced by Zoosk on June 3, 2020, who paid for subscriptions with Zoosk (as to monetary relief under Rule 23(b)(3) for the UCL claim)
- **California Subclass**: All individuals whose PII was compromised in the Data Breach announced by Zoosk on June 3, 2020, who reside in California (in the alternative, should either of the two above classes be limited to California residents only).

A. THE PROPOSED CLASSES MEET RULE 23(a) REQUIREMENTS

1. With [redacted] Users Breached, Numerosity is Met

Zoosk concedes that [redacted] were compromised. Zoosk's Amended Resp. to Plfs' 1st Interrog., Resp. No. 10, p. 18. Zoosk reported to the credit bureaus that approximately [redacted] United States residents were impacted. *See* ZOOSK0000818, 828, 834, attached as **Composite Exhibit H**. The Subscription Subclass is composed of more than [redacted]. *See* Expert Report of Gary Olsen at ¶¶ 3, 9; Olsen Schedules 3 & 5, attached as **Exhibit I**. Thus, the proposed class is sufficiently numerous. *Rannis v. Recchia*, 380 F. App'x 646, 651 (9th Cir. 2010) (noting numerosity usually met with at least 40 class members).[19]

[19] The proposed class members will be readily ascertainable from Zoosk's records. Plaintiff does not address this any further in light of *Briseno v. Con Agra Foods, Inc.*, 844 F. 3d 1121, 1133 (9th Cir. 2017).

2. Zoosk's Conduct Related to The Breach Raises Common Legal and Factual Questions

Rule 23(a)(2) requires "questions of law or fact common to the class." A single common question is sufficient. *See Ellis*, 657 F.3d at 981. A common question is one that "generate[s] common answers apt to drive the resolution of the litigation." *Torres v. Mercer Canyons Inc.*, 835 F. 3d 1125, 1133 (9th Cir. 2016). The claims here easily meet this standard. Each Class member's PII was compromised due to the same security vulnerabilities. Therefore, proof of what Zoosk knew about its vulnerabilities and what it did or did not do to address them is common to all class members. The requisite commonality exists here because the issues raised by the class's claims have common answers that will drive the resolution of this case. These include:

- Whether Zoosk owed a duty to exercise due care in collecting, storing, and safeguarding PII;
- Whether Zoosk breached that duty;
- Whether Zoosk knew about the security risk posed by its security vulnerabilities (and when);
- Whether Zoosk's failure to remedy obvious and known security risks was affirmative negligence;
- Whether by failing to adequately investigate the Breach while it was underway and after its discovery, Zoosk committed affirmative negligence;
- Whether Zoosk's security is still inadequate to protect user PII; and
- Whether Zoosk's conduct was in violation of the UCL.

These types of common questions have been found sufficient to support class certification in prior data breach cases such as *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 19-MD-2879, 2022 WL 1396522, at *10 (D. Md. May 3, 2022) (hereinafter "*Marriott Data Breach*") and *In re Brinker Data Incident Litig.*, 3:18-CV-686-TJC-MCR, 2021 WL 1405508, at *8 (M.D. Fla. Apr. 14, 2021).

3. Plaintiff's Claims are Typical of the Class

Rule 23(a)(3)'s typicality standard is met when the class representative's claims arise from the same course of events and rely on similar legal arguments as other class members' claims. *Parsons v. Ryan*, 754 F.3d 657, 685 (9th Cir. 2014). These claims "need not be substantially identical." *Hanlon v. Chrysler Corp.*, 150 F.3d 1101, 1020 (9th Cir. 1998). Plaintiff's PII was compromised in the same Breach as was the PII of other class members. Thus, typicality is necessarily satisfied where, as here, "the plaintiff endured a course of conduct directed against the class." *Just Film v. Buono*, 847 F.3d 1108, 1118 (9th Cir. 2017).

Plaintiff Greenamyer's claims and legal theories, in her individual and representative capacities, arise under the same factual predicate. *See* Declaration of Tracy Greenamyer, attached as **Exhibit J**, at ¶¶ 2–3. The elements Plaintiff must prove for negligence and violation of the UCL are identical to what absent class members would need to prove, and there are no defenses unique to Plaintiff Greenamyer.[20] Plaintiff's affirmative negligence and UCL claims are also typical to the nationwide class because, like all class members, she was harmed by Zoosk's information security vulnerabilities and its failure to remedy the vulnerabilities despite long-term knowledge of their existence. In other words, she was subject to the same decision-making as were other Class members. Plaintiff, and class members, face the same risk of identity theft (negligence), same subscription fee overpayment (UCL claim), and same need for future protection of their PII (injunctive relief).

4. Plaintiff and Proposed Class Counsel are Adequate

Rule 23(a)(4) requires the class representative to "fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). Adequacy is satisfied when 1) the named plaintiff and counsel have no conflicts with the class; and 2) plaintiff will "prosecute the action vigorously." *Staton v. Boeing Co.*, 327 F.3d 938, 957 (2003); *see also* Fed. R. Civ. P. 23(a)(4). Plaintiff has no conflicts

[20] Certification and appointment as a class representative is not sought on behalf of Plaintiff Flores-Mendez because of potentially unique, and individualized, issues concerning the manner in which his subscription fees were paid. Proposed Class Counsel believe this, among other issues, bear on Plaintiff Flores-Mendez's typicality and adequacy and hence do not seek his appointment as a class representative here.

with the class, and instead shares the same interests in prosecuting these claims. She has participated actively in this case, including by reviewing pleadings, responding to discovery, and sitting for deposition. Greenamyer Decl. ¶ 4.

Proposed class counsel—John Yanchunis, Ryan McGee, Patrick Barthle, and Kiley Grombacher—are experienced class action attorneys and are committed to prosecuting this case. *See* Declarations of Proposed Class Counsel, attached as **Composite Exhibit K**. To date, proposed class counsel have, among other things: 1) propounded and responded to discovery and engaged in discovery motion practice; 2) argued motions to dismiss and amend the pleadings; 3) reviewed and coded documents; 4) deposed four former Zoosk employees, with two such depositions occurring in Germany; 5) deposed Zoosk's corporate representatives under Rule 30(b)(6); 6) engaged a cybersecurity expert to opine on Zoosk's negligent security practices, and appropriate equitable relief to change those practices; and 7) engaged a financial expert to provide models for Subscription Subclass members' recovery. Thus, Plaintiff and proposed Class Counsel meet the adequacy requirement.

B. THE COURT SHOULD CERTIFY A 23(b)(2) CLASS

Class certification of a claim for declaratory or injunctive relief is appropriate when, in addition to the four requirements of Rule 23(a) discussed above, "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief … is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). "Unlike Rule 23(b)(3), a plaintiff does not need to show predominance of common issues or superiority of class adjudication to certify a Rule 23(b)(2) class." *Yahoo Mail*, 308 F.R.D. at 587; *see also Brazil v. Dole Packaged Foods, LLC*, 2014 WL 2466559, at *10 (N.D. Cal. May 30, 2014) ("Ordinarily, it follows that there is no need [in evaluating a Rule 23(b)(2) class] 'to undertake a case-specific inquiry into whether class issues must predominate or whether class action is the superior method of adjudicating the dispute [.]'").

Indeed, "[w]hen a class seeks an indivisible injunction benefiting all its members at once, there is no reason to undertake a case-specific inquiry into whether class issues predominate or whether class action is a superior method of adjudicating the dispute." *Wal-Mart Stores, Inc. v.*

Dukes, 564 U.S. 338, 362–63 (2011). Accordingly, the "key to the (b)(2) class is 'the indivisible nature of the injunctive or declaratory remedy warranted—the notion that the conduct is such that it can be enjoined or declared unlawful only as to all of the class members or as to none of them.'" *Dukes*, 564 U.S. at 360 (quoting Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. Rev. 97, 132 (2009)).

Thus, Rule 23(b)(2) applies "when a single injunction or declaratory judgment would provide relief to each member of the class. It does not authorize class certification when each individual class member would be entitled to a *different* injunction or declaratory judgment against the defendant." *Dukes*, 564 U.S. at 360–61 (emphasis in original).

"Any person who engages, has engaged, or proposes to engage in unfair competition may be enjoined in any court of competent jurisdiction." Cal. Bus. & Prof. Code §17203. Any person who has suffered injury in fact and lost money or property as a result of unfair competition "may pursue representative claims or relief on behalf of others." *Id.*; *see also id.* at §17204.

Here, Plaintiff's negligence and UCL relief claims meet that standard because Zoosk acted in a manner common to the Class. Zoosk subjected all Class members' PII to the same security vulnerabilities; Class members' PII was compromised as a result of those vulnerabilities; Zoosk is still in possession of Class members' PII; and Zoosk still has not adequately secured the PII. *See, e,g,* Strebe Decl ¶¶ 133–139. Injunctive relief is thus needed to remediate Zoosk's inadequate security, which uniformly applies to all Class members.

Because Zoosk's company-wide policies and failures were uniform and persistent through the entire relevant time period, and continue to significantly increase the risk of harm to all class members, Rule 23(b)(2) certification is particularly apt. *See Parsons v. Ryan*, 754 F.3d 657, 688 (9th Cir. 2014) (affirming certification seeking injunction of systemic deficiencies in policies and practices that put all plaintiffs at substantial risk of harm). *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686 (N.D. Cal. 2019) is instructive. There, as here, "plaintiff [sought] injunctive relief to impose a set of changes on Facebook's conduct to ensure no further harm comes to him and the class." *Id.* at 698. This Court agreed, finding: "the requested relief of an order compelling Facebook to

promptly correct any problems or issues detected by such third-party security auditors outlines the 'general contours' of the requested injunction at this stage. A more specific remedy can be fashioned later in this litigation. Facebook ultimately has not sufficiently shown otherwise that 'crafting uniform injunctive relief will be impossible.'" *Id.* at 698. The same is true here.

Plaintiff's expert Matthew Strebe has set forth the security controls needed to protect class members' PII in the future. These include:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted];
- [redacted];
- [redacted];
- [redacted]; and
- [redacted]

See Strebe Decl. at ¶¶ 138–139.

C. RULE 23(b)(3) CERTIFICATION OF THE SUBSCRIPTION SUBCLASS IS PROPER

There is "clear justification for handling the dispute on a representative . . . basis if common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication." *In re Lenovo Adware Litig.*, 2016 WL 6277245, at *17 (N.D. Cal. Oct. 27, 2016) (internal citations omitted). The common questions can be resolved in one fell swoop, as demonstrated below.

1. Common Questions of Law and Fact Predominate

"The predominance analysis under Rule 23(b)(3) focuses on the relationship between the common and individual issues in the case, and 'tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation.'" *Just Film*, 847 F.3d at 1120 (internal citations omitted). It generally begins with an examination of the elements underlying a plaintiff's causes of action. *Ellsworth v. U.S. Bank, N.A.*, 2014 WL 2734953, at *19 (N.D. Cal. June 13, 2014). "In determining whether common questions predominate, the Court identifies the substantive issues related to plaintiff's claims (both the causes of action and affirmative defenses); then considers the proof necessary to establish each element of the claim or defense; and considers how these issues would be tried." *Id.* Where, as here, the conduct giving rise to both the duty and breach is uniform, Plaintiff's negligence claim is appropriate for classwide resolution as questions of legal duty and Zoosk's breach of that duty are common issues susceptible to common proof.[21] *See Giroux v. Essex Prop. Tr., Inc.*, 2018 WL 2463107, at *4 (N.D. Cal. June 1, 2018); *see, e.g.*, *Smith v. Triad of Alabama, LLC*, 2017 WL 1044692, at *13 (M.D. Ala. Mar. 17, 2017) (certifying negligence class in data breach suit against hospital where each class member was a "non-hospital" patient at the hospital, alleged injury as a result of a rogue employee's theft of records, suffered the same general type of damages, and class members' claims were subject to a single state's law), *aff'd on reconsideration*, 2017 WL 3816722 (M.D. Ala. Aug. 31, 2017).

UCL § 17200 prohibits acts or practices that are (1) unlawful, (2) unfair, or (3) fraudulent. Each of the foregoing prongs permits a separate theory of relief. *See Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1168 (9th Cir. 2012). "[A] breach of contract may form the predicate for a section 17200 claim, provided it also constitutes conduct that is unlawful, or unfair, or fraudulent." *Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1152 (9th Cir. 2008) (cleaned up).

Although the UCL "require[s] plaintiffs to prove members of the public are likely to be deceived by the defendant's business practices," *Williams v. Gerber Prods. Co.*, 552 F.3d 934, 938

[21] Plaintiff seeks certification of her negligence claim only under Rule 23(c)(4), as explained further below, and only as to the issues of duty and breach. However, to whatever extent predominance analysis applies to issue certification, that analysis is referenced here.

(9th Cir. 2008), plaintiffs' burden of proof is modest. *Friedman v. AARP*, 855 F.3d 1047, 1055 (9th Cir. 2017). It is subject only to an objective "reasonable consumer standard," *id*., not implicating individual issues specific to each consumer. *Lilly v. Jamba Juice Co*., 308 F.R.D. 231, 242 (N.D. Cal. 2014); *see Kumar v. Salov N. Am. Corp*., 2016 WL 3844334, at *7 n.9 ("Claims under the UCL . . . do not require[] individualized proof of reliance, deception, or causation.").

"[A]n inference of common reliance arises if representations are material." *Lilly*, 308 F.R.D. at 242. The test for materiality is whether "'a reasonable man would attach importance to its existence or nonexistence in determining his choice of action in the transaction.'" *Mullins*, 2016 WL 1535057, at *5. "As materiality is an objective inquiry, no individualized examination of materiality is necessary." *Lanovaz v. Twinings N. Am., Inc*., 2014 WL 1652338, at *4 (N.D. Cal. Apr. 24, 2014). "As a general rule, materiality may be established by common proof." *Mullins*, 2016 WL 1535057, at *5; *see also Amgen Inc. v. Conn. Ret. Plans & Tr. Funds*, 133 S. Ct. 1184, 1191 (2013) ("Because materiality is judged according to an objective standard, the materiality of [defendant's] alleged misrepresentations and omissions is a question common to all members of the class . . . .").

Plaintiffs are not required to "'produce a consumer survey or similar extrinsic evidence to prevail on a claim that the public is likely to be misled by a representation.'" *Mullins*, 2016 WL 1535057, at *5. "'While a plaintiff must show that the misrepresentation was an immediate cause of the injury-producing conduct, the plaintiff need not demonstrate it was the only cause.'" *Mullins*, 2016 WL 1535057, at *5.

And, the classwide exposure element of reliance under the UCL is easily established here, where all Subscription Subclass members were required to "agree and consent" to Zoosk's privacy policy. As this Court already found: "Zoosk's own terms prove that [ ] plaintiffs consented to the privacy policy. *Read and consented to* means *understood*." (ECF No. 133 at 5) (emphasis in original); *see also Mullins*, 2016 WL 1535057, at *2.

a. Reliance is Not an Obstacle to Certification of the UCL

The Court here previously observed that "a Section 17200 claim theorizing that plaintiffs read and considered alleged misrepresentations, the claim generally must plead 'actual reliance.'" (ECF No. 133 at 4) (citing *In re Tobacco II Cases*, 46 Cal.4th 298, 324–26 (2009)). Plaintiff asserts

that where a defendant breaches contractual privacy protections governing the relationship it has with its users, there is no requirement of reliance, and those affected users have standing under the UCL. *Cappello v. Walmart Inc.*, 394 F. Supp. 3d 1015, 1020 (N.D. Cal. 2019) (Seeborg, J.). Moreover, a defendant that "systematically breach[es] its Privacy Policy . . . contravenes California's well-established public policy of protecting consumer data, as reflected in Section 22576 and other statutes. District courts have found similar allegations sufficient to plead 'unfair' conduct under the balancing test." *Id.* at 1024 (citing *Svenson v. Google, Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429, at *10 (N.D. Cal. April 1, 2015); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1227 (N.D. Cal. 2014); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-md-02752-LHK, 2017 WL 3727318, at *24 (N.D. Cal. Aug. 30, 2017)).

In ruling on Plaintiffs' Motion to Amend, this Court recognized:

> Zoosk's own terms prove that that plaintiffs consented to the privacy policy. *Read and consented to* means *understood*. And, Flores-Mendez has alleged that he would have cancelled his subscription had Zoosk disclosed its true data-security practices (Proposed Third Amd. Compl. ¶ 47). *See Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 330 (2011) (alleging the plaintiff "would not have bought the product but for" the unfair business practice). Our allegedly misleading statements, which relate to data security, feature centrally in the privacy policy as a whole. For both of these reasons, **a presumption arises that average subscribers would find them important enough to affect their decision to purchase**. Note that it does not matter that all customers were presumed to agree to the policy upon sign up, but that Flores-Mendez subsequently decided to purchase the subscription. Critically, at the time of purchase, it's alleged that Zoosk had already presumed that Flores-Mendez knew of and consented to the privacy policy. Thus, Flores-Mendez has sufficiently alleged a loss of money or property as a result of the alleged Section 17200 violation.

(ECF No. 133 at 5–6) (bold emphasis added). Accordingly, individual, subjective need not be shown here for class certification purposes.[22]

[22] This Court's prior order expressly noted that "[s]ince this order has found standing adequately alleged, it does not reach the dispute over whether a complaint alleging a breach-of-contract theory of standing also requires proof of reliance on an alleged misrepresentation in that contract." (ECF No. 133 at 7). To whatever extent necessary, Plaintiff reasserts those arguments again here.

This Court likewise previously found Plaintiff's UCL claim viable under the unfair prong, based on Zoosk's "misleading statements coupled with Zoosk's failure to disclose its 'inadequate' data-security practices," along with Zoosk's "fail[ure] to apply subscription customers' funds to data-security practices" despite Plaintiff's expectations to the contrary. (ECF No. 133 at 8–9).

As explained above and in the declaration of Plaintiff's cybersecurity expert Matt Strebe, Zoosk's data-security practices were inadequate in a number of ways, including [redacted] Strebe Decl. § V.

b. Damages Have Been Established with Common Proof and Calculated with Common Methodologies.

Zoosk produced data files in this case identifying, by user ID number, every member of the Subscription Subclass, along with subscription fee payment information for those Subscription Subclass members. Olsen Report ¶ 8, Olsen Schedules 3 – 5.[23] Zoosk also provided certain audited financial statements. *See* Olsen Report Schedule 6z. From these data sources, Plaintiff's expert Gary Olsen has calculated Subscription Subclass damages in three ways:

a. **Calculation 1**—Zoosk received [redacted] in total revenue from the Subscription Subclass from 2015 to 2020;

[23] This data also identifies which Subscription Subclass members are also California residents, if the Court believes the class must be so limited. Plaintiff does not believe so based on Zoosk's California choice-of-law provision in its Terms of Services, which mandates that the internal substantive laws of the State of California shall govern, irrespective of a consumers' residency. *See, e.g.*, Zoosk's Terms of Service (September 7, 2016 revision).

b. **Calculation 2**—Zoosk received profits of [redacted] from the Subscription Subclass; and

c. **Calculation 3**—Zoosk inappropriately retained a portion of the profits from the Subscription Subclass totaling [redacted] as a result of not spending sufficient amounts on data security.

Olsen Report ¶ 3.

Calculation 1 rests on the premise that Plaintiff and the Subscription Subclass are entitled to a return of all subscription fees as damages because had they known about Zoosk's inadequate data security, they would have used another service and not paid these fees to Zoosk. Olsen Report ¶ 14.

Calculation 2 computes profits derived from that total revenue by considering the direct costs and sales and marketing costs necessary to generate those revenues. Zoosk's direct costs of revenue were between [redacted] of its revenues, depending on the year reviewed. Olsen Report ¶ 17, Schedule 6. These percentages were applied to the respective revenues received from the Subscription Subclass from 2015 to January 2020. In addition, Zoosk appears to have incurred significant marketing and sales expenses that were used to generate its revenues. These sales and marketing costs ranged from [redacted] of Zoosk's revenues. These ratios were likewise applied to the respective Subscription Subclass revenues received from 2015 to January 2020. Olsen Report ¶ 17. Applying these cost ratios from Zoosk's financial statements to the revenue it received from the Subscription Subclass, and subtracting those estimated costs from that revenue, results in approximately $[redacted] in inappropriately retained profits that Plaintiff seeks as damages for the UCL claim. Olsen Report ¶ 18.

Finally, should the Court be of the view that only the portion of subscription fee profits that should have been spent on information security is recoverable for this claim, Calculation 3 has, based on discovery in this case and independent research, estimated an appropriate level of data security spend for Zoosk at $[redacted] from 2015 to 2020.[24] Olsen Report ¶ 20. Because the

[24] Notably, Zoosk did not provide sufficient information to determine the actual amount it spent on data security. Olsen Report ¶ 20. The additional financial information Zoosk provided just prior to the expert report deadline was so replete with issues as to prevent meaningful analysis. *Id.* ¶ 24.

revenue reported by Zoosk for the Subscription Subclass represents approximately [redacted] of Zoosk's total revenue, this ratio was applied to the total amount that Zoosk should have spent on data security, resulting in [redacted] in data security non-spend attributable to the Subscription Subclass. Olsen Report ¶ 22.

In any event, regardless of the methodology, each can easily be applied class-wide, militating in favor of certification.

2. A Class Action is Superior to Millions of Expensive Trials

Certification of the Subscription Subclass's UCL claim would be "superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). Indeed, this is the kind of case for which the class action procedure was created. First, any Subscription Subclass member's individual recovery, would be dwarfed by the cost of proving the predominating issues in this litigation. *Soares v. Flowers Foods, Inc.*, 320 F.R.D. 464, 485 (N.D. Cal. 2017) (Rule 23(b)(3)(A) "only weighs against class certification where individual damages 'run high' such that individual class members have a strong interest 'in making individual decisions on whether and when to settle'"). "[T]his case 'is the classic negative value case; if class certification is denied, class members will likely be precluded from bringing their claims individually because the cost to bring the claim outweighs the potential payout.'" *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 2022 WL 1396522, at *27 (quoting *Brinker*, 2021 WL 1405508, at *13)).

Second, no separate cases exist outside this proceeding indicating low or no interests to pursue the matter on an individual basis. *See* Fed R. Civ. P. 23(b)(3)(B). Third, Zoosk's Terms of Service dictate all litigation must be brought in Santa Clara County, California, USA, highlighting the desirability of concentrating the litigation in this forum. *See* Fed. R. Civ. P. 23(b)(3)(C). Finally, the issues presented in this class litigation are manageable in light of the known users and application of California law. *See* Fed. R. Civ. P. 23(b)(3)(D). A class action provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Individualized litigation would create a potential for inconsistent or contradictory judgments on the issues Plaintiff

---

Should Zoosk provide the missing data, Mr. Olsen reserves the right to amend his conclusions. *Id.*

seeks to certify here (including, most notably, whether Zoosk took adequate measures to protect users' PII) and would increase the delay and expense to all parties and the court system.

Notice should not be cumbersome. Each class member can be contacted directly by email using Zoosk's records. *See* Fed. R. Civ. P. 23(c)(2)(b). Otherwise, notice via publication through a variety of means may be used for class members who no longer have their Zoosk accounts, and/or whose email addresses are no longer active. Further, because the Breach has been publicized around the world, a public notice in the U.S. would be effective.

Last, because class members can easily be verified using data maintained by Zoosk—which has already identified Subscription Subclass members by user ID and notified all class members concerning the Breach—the notice process will be straightforward. *Id.* Thus, while ascertainability is not a requirement in the Ninth Circuit, *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1133 (9th Cir. 2017), the manageability problems that sometimes plague certification do not exist here.

D. THE COURT SHOULD ALSO CERTIFY COMMON ISSUES UNDER RULE 23(C)(4)

"When appropriate," Rule 23(c)(4) allows a court great discretion to certify an action "as a class action with respect to particular issues." Fed. R. Civ. P. 23(c)(4). It does not prescribe elements that representatives must show in order to maintain an issue class, but courts recognize its value in resolving cases where, though common questions may not predominate, denying certification of common issues would all but strip class members of their right to seek relief.

The Ninth Circuit has endorsed the use of issue certification. *Valentino*, 97 F.3d at 1234. So have many other circuit courts. *See In re Deepwater Horizon*, 739 F.3d 790, 817 (5th Cir. 2014); *Butler v. Sears, Roebuck & Co.*, 727 F.3d 796, 800 (7th Cir. 2013); *In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig.*, 722 F.3d 838, 860 (6th Cir. 2013); *see also Jimenez II*, 765 F.3d at 1168 (noting *Butler, Whirlpool, and Deepwater Horizon* "are compelling . . .[a]nd their reasoning is consistent with our circuit precedent"). As explained above, basic liability questions predominate for Plaintiff's negligence claims. *Tasion Commc'ns, Inc. v. Ubiquiti Networks, Inc.*, 308 F.R.D. 630, 633 (N.D. Cal. 2015). The Court may certify issues under Rule 23(c)(4) if it materially advances the litigation as a whole, with the focus being "judicial economy and

efficiency." *Kamakahi v. Am. Soc'y for Reprod. Med.*, 305 F.R.D. 164, 193 (N.D. Cal. 2015) (internal citations omitted). Importantly, the analysis focuses only on the issues to be certified. *See Deane v. Fastenal Co.*, 2012 WL 12552238, at *7 (N.D. Cal. Sept. 26, 2012).

A common trial on liability—specifically, the issues of duty and breach for the negligence claim—of Zoosk for the Breach would materially advance the litigation. *Loritz v. Exide Techs., Inc.*, 2015 WL 6790247, at *24 (N.D. Cal. July 21, 2015). This approach was recently adopted in the *Marriott Data Breach* case, where the court, in additional to certifying several claims under Rule 23(b)(3), as noted above, also certified under Rule 23(c)(4), finding that "common issues will predominate over any individual questions as to the duty and breach elements of negligence . . . ." *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 2022 WL 1396522, at *31. The same is true here. Establishing duty and breach for Plaintiff's negligence claim can be done on a class wide basis. If successful, class members can then seek recovery in follow-on proceedings of more individualized damages, such as time spent responding to the data breach, cost of mitigation measures, and out-of-pocket fraud losses, "which are the relevant theories of harm" in this analysis, and for which "individualized issues related to causation are quite significant," but which only buttresses the need for issue certification. *Id*. at *30.

Further, "Courts retain discretion to shape the proceedings and could ultimately choose an option such as the use of individual claim forms or the appointment of a special master, which plainly would allow [d]efendants to raise any defenses they may have to individual claims." *Jimenez v. Allstate Ins. Co.*, 765 F.3d 1161, 1168-69 (9th Cir. 2014) ("*Jimenez II*") (finding "statistical analysis [was] capable of leading to a fair determination of [defendant's] liability" and individualized damages hearings "preserved the rights of [defendant] to present its damages defenses on an individual basis"). The issues for trial would solely relate to Zoosk's conduct—did it owe a duty in negligence and was that duty breached; with individual follow-on proceedings for those seeking individual damages. If the answer to one or more of the questions is "No," then the litigation ends. If the answers are "Yes," then all remaining issues are capable of adjudication through a streamlined process that is far superior to requiring users to independently establish what

Zoosk did (or did not) do to safeguard PII and what Zoosk knew and when. Thus, the answers would help to efficiently resolve the litigation.

V. CONCLUSION

For the reasons stated herein, the Court should grant Plaintiff's Motion to For Class Certification; appoint Plaintiff Greenamyer as the Class Representative; appoint John Yanchunis, Ryan McGee, Patrick Barthle, and Kiley Grombacher as Class Counsel; and direct that notice be provided to the Class.

Dated: May 20, 2022

Respectfully submitted,

BRADLEY/GROMBACHER, LLP
CROSNER LEGAL P.C
MORGAN & MORGAN
COMPLEX LITIGATION GROUP

By: /s/ Kiley L. Grombacher
Marcus J. Bradley, Esq.
Kiley L. Grombacher, Esq.
Lirit A. King, Esq.
Zachary M. Crosner
Michael R. Crosner
John A. Yanchunis